



Please type a plus sign (+) inside this box →

PTO/SB/05 (4/98)

Approved for use through 09/30/2000. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No. NCI-061

First Inventor or Application Identifier Xiao, Peter et al

Title Hierarchical Open Security Information Delegation and Acquisition

Express Mail Label No. EJ 788 581 029 US

## APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1.  \* Fee Transmittal Form (e.g., PTO/SB/17)  
(Submit an original and a duplicate for fee processing)

2.  Specification [Total Pages 27]  
(preferred arrangement set forth below)

- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3.  Drawing(s) (35 U.S.C. 113) [Total Sheets 9]

4. Oath or Declaration [Total Pages ]

- a.  Newly executed (original or copy)
- b.  Copy from a prior application (37 C.F.R. § 1.63(d))  
(for continuation/divisional with Box 16 completed)
- i.  DELETION OF INVENTOR(S)  
Signed statement attached deleting  
inventor(s) named in the prior application,  
see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

\* NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

ADDRESS TO: Assistant Commissioner for Patents  
Box Patent Application  
Washington, DC 20231

- 5.  Microfiche Computer Program (Appendix)
- 6. Nucleotide and/or Amino Acid Sequence Submission  
(if applicable, all necessary)
  - a.  Computer Readable Copy
  - b.  Paper Copy (identical to computer copy)
  - c.  Statement verifying identity of above copies

## ACCOMPANYING APPLICATION PARTS

- 7.  Assignment Papers (cover sheet & document(s))
- 8.  37 C.F.R. § 3.73(b) Statement  Power of  
(when there is an assignee)  Attorney
- 9.  English Translation Document (if applicable)
- 10.  Information Disclosure Statement (IDS)/PTO-1449  Copies of IDS  
Statement (IDS)/PTO-1449  Citations
- 11.  Preliminary Amendment
- 12.  Return Receipt Postcard (MPEP 503)  
(Should be specifically itemized)
- 13.  \* Small Entity Statement(s)  Statement filed in prior application,  
(PTO/SB/09-12)  Status still proper and desired
- 14.  Certified Copy of Priority Document(s)  
(if foreign priority is claimed)
- 15.  Other:   
.....  
.....

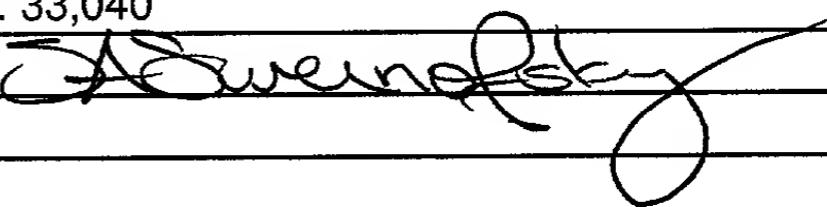
## 16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

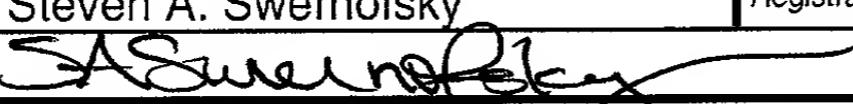
Continuation  Divisional  Continuation-in-part (CIP) of prior application No: \_\_\_\_\_ / \_\_\_\_\_

Prior application information: Examiner \_\_\_\_\_ Group / Art Unit: \_\_\_\_\_

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

## 17. CORRESPONDENCE ADDRESS

<input type="checkbox"/> Customer Number or Bar Code Label	(Insert Customer No. or Attach bar code label here)			or	<input type="checkbox"/> Correspondence address below
Name	Steven A. Swernofsky			Reg. No. 33,040	
	The Law Offices of Steven A. Swernofsky				
Address	Post Office Box 390013				
City	Mountain View	State	CA	Zip Code	94039-0013
Country	USA	Telephone	650-947-0700	Fax	640-947-8438

Name (Print/Type)	Steven A. Swernofsky	Registration No. (Attorney/Agent)	33,040
Signature		Date	June 11, 1999

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

JC551 U.S. PTO  
09/330214  
06/11/99

1           This application is submitted in the name of the following inventors:

2

3 <u>Inventor</u>	4 <u>Citizenship</u>	5 <u>Residence City and State</u>
6    Xiao, Peter	7    Peoples Republic of China	8    Fremont, California
9    Quilice, Jeffrey	10   United States	11   Mountain View, CA
12   Swart, Garrett	13   United States	14   Palo Alto, CA
15   Valente, Luis	16   Canada	17   Mountain View, CA

18

9           The assignee is Network Computer, Inc., having an office at 1000 Bridge  
10   Parkway, Redwood Shores, CA 94065.

11

12           Title of the Invention

13

14           Hierarchical Open Security Information Delegation and Acquisition

15           Cross-Reference to Related Applications

16

17           This application claims priority of the following applications:

18

19   o       Application No. 08/770,238, filed December 20, 1996, in the name of inventors  
20       Wei Yen and Steven Weinstein, titled "Internet Multiplexer for Broadcast and  
21       Other Information", attorney docket NAV-001;

1 o Provisional Application Serial No. 60/046,748, filed May 16, 1997, in the name of  
2 inventors Luis Valente, Venkatachary Srinivasan, Andreas Atkins and Wei Ling  
3 Chu, titled "Client Server Architecture," attorney docket number NAV-008P.

4

5 o Application Serial No. 09/080,571, filed May 18, 1998, in the name of inventors  
6 Luis Valente, Venkatachary Srinivasan, Andreas Atkins and Wei Ling Chu, titled  
7 "Security Information Acquisition," attorney docket number NCI-008A.

8

9 o Application Serial No. 09/162,650, filed September 29, 1998, in the name of Luis  
10 Valente, titled "Security Information Acquisition" attorney docket number NCI-  
11 055.

12

13 These applications are referred to herein as the "Incorporated Disclosures,"  
14 and are hereby incorporated by reference as if fully set forth herein.

15

16 Background of the Invention

17

18 1. *Field of the Invention*

19

20 This invention relates to computer security.

21

1    2.    *Related Art*

2  
3            In a data delivery system, data receivers need to know whether they can  
4            trust information they receive from senders. This need is increasing due to the growth of  
5            data exchanges and business transactions taking place on the Internet over non-secure  
6            communication links.

7  
8            The growing Public Key Infrastructure ("PKI") provides a way for  
9            receivers of data to know whether they can trust information they receive from senders.  
10           In the PKI, trusted third parties issue digital certificates ("public key certificates") that  
11           attest to the authenticity of the binding of a public key to its owner. These trusted third  
12           parties are known as certification authorities "CAs", or sometimes are called "public  
13           CAs" if their services are available to the public. These digital certificates are created  
14           and used using known encryption and decryption security techniques. Verisign, Inc. is an  
15           example of a public CA. Senders obtain a certificate from a CA, and include the  
16           certificate with the data they wish to send to the receiver. The certificate includes enough  
17           information for the receiver to verify that the sender's self-identification is accurate  
18           (verification of identity), and that the data was not compromised between the sender and  
19           the receiver (validation of contents).

20  
21           The PKI has the general drawback that digital certificates accepted by the  
22           receiver are limited to those from certification authorities that the receiver already trusts.

1 Thus the general problem of providing trust information to the receiver is inherent in the  
2 PKI. The trust information required by the receiver can include the identities of trusted  
3 senders, for what purpose the senders are trusted, and sufficient information to  
4 authenticate messages from the trusted senders.

5

6 For instance, Secure Socket Layer ("SSL) is a widely adopted protocol that  
7 is used within the PKI for authentication and encryption. To authenticate a message, the  
8 client must have enough trust information regarding the digital certificate sent by the SSL  
9 server ("server certificate")--at a minimum the client must have an authentic copy of the  
10 certificate of the CA who issued the SSL server certificate. However, computers,  
11 particularly in the consumer market, have limited resources, including limited nonvolatile  
12 storage, to store such information.

13

14 A computer administrator must decide which CAs to trust. In the case of  
15 personal computers used in homes or small offices, the user may be unsophisticated,  
16 lacking in knowledge, or unwilling to make and implement his trust decisions. A  
17 common solution is providing a factory-defined set of trust relationships. This makes the  
18 security measures transparently available to the user. However it is impractical for  
19 inexpensive personal computing devices due to the high cost of nonvolatile memory. In  
20 addition this solution provides a static set of trust relationships, and does not provide for  
21 updates.

22

1           The Incorporated Disclosures provide a method for a computing device to  
2 acquire trust information after it is manufactured. These applications disclose the general  
3 approach of using Security Information Objects ("SIOs"), with a single Trusted Security  
4 Information Provider (or at least a single level of TSIPs) defining the trust relationship for  
5 all parties. One drawback of the method disclosed is only the TSIP can issue an SIO.  
6 Furthermore, the TSIP must administer all parties's trust information, when the TSIP may  
7 only be interested in detailed definition of the trust relationship between the TSIP and its  
8 closest business partners. Yet, the TSIP may wish to retain some general control over  
9 what other partners can do.

10  
11           In addition, complex interrelated business relationships exist and are  
12 evolving on the Internet, and it is desirable to design a system that will also provide  
13 accountability and enforcement of complex business relationships and rules. An example  
14 business hierarchy is shown in FIG. 1, and is discussed in detail in the Detailed  
15 Description below. Referring to FIG. 1, using the method disclosed in the Incorporated  
16 Disclosures, OEM1 and OEM2 would be indistinguishable to ISP1 and ISP2. However,  
17 it may be desired to distinguish between OEM1 and OEM2, for instance so that if ISP1 is  
18 a client of OEM1, it can be prevented from subscribing to services of OEM2. Or, so  
19 OEM2 cannot steal customers of OEM1.

20  
21           Accordingly, it would be advantageous for a security system to provide a  
22 way for each business party to dynamically provide trust information to its clients based

1 on its own business and security requirements, while centralized control is maintained  
2 where desired. The system would be transparent to the end-user, and would be easy to  
3 implement.

4

5                   The invention provides a Hierarchical Open Security Information  
6 Delegation and Acquisition System which allows secure and dynamic distribution of  
7 security information to multiple clients over non-secure channels. It also allows parties  
8 to modify the security information, within boundaries that are set by higher-level parties.  
9 Such modification can include adding third-party CAs to the list of entities trusted to  
10 issue SSL certificates. It provides a technique for each business party to define its own  
11 trust relationships with other entities including public CAs, within the parameters that are  
12 hierarchically set.

13

14                   Summary of the Invention

15                   The invention provides a method and system for secure data transfer and  
16 dynamic definition of trustworthiness of various entities by multiple parties in a hierarchy  
17 tree or graph structure. The invention uses digital certificates. Each party in the  
18 business hierarchy can control and define various trust information including  
19 trustworthiness and delegation authority for the entities it deals with. The ability of a  
20 party to redefine or add trust information is controlled by the parties with which it has a  
21 relationship that are above it in the hierarchy. Trust vectors and delegation vectors are  
22 used to store this information. Each party can add trusted third parties to a security

1 object without compromising the integrity of security objects already issued. A sequence  
2 of security objects including digital certificates can be modified without compromising  
3 the original digital certificates in those security objects

4

5 Brief Description of the Drawings

6

7 FIG. 1 shows an example business hierarchy.

8 FIG. 2 shows the general format of an X509 version 3 certificate.

9 FIG. 3 shows a schematic of root certificate chaining.

10 FIG. 4 shows a sample Root Security Information Object for an OEM.

11 FIG. 5 shows sample values given to bits in the trust-delegation vector.

12 FIG. 6 shows a schematic of how an HSIO chain of RSIOs is linked.

13 FIG. 7 shows a process flow diagram for a client to validate a Hierarchical  
14 Security Information Object.15 FIG. 8 shows a process flow diagram whereby an SSL server certificate can  
16 be authenticated.

17

18 Detailed Description of the Preferred Embodiment

19 In the following description, a preferred embodiment of the invention is  
20 described with regard to preferred process steps and data structures. Those skilled in the  
21 art would recognize after perusal of this application that embodiments of the invention  
22 can be implemented using one or more general purpose processors or special purpose

1 processors or other circuits adapted to particular process steps and data structures  
2 described herein, and that implementation of the process steps and data structures  
3 described herein would not require undue experimentation or further invention.

4

5           Alternative embodiments may use other and further forms of authentication  
6 and certification, using other forms of cryptography either in addition to or instead of  
7 public key cryptography, and are within the scope and spirit of the invention.

8

9           Inventions disclosed herein can be used in conjunction with inventions  
10 disclosed in the Incorporated Disclosures, referenced previously.

11

12       *Overview of the Invention*

13

14           The invention provides a secure and dynamic way of distributing trust  
15 information from a centralized authority to parties in a hierarchy that have a relationship  
16 with it. Among other things, it provides client with enough information to identify  
17 trusted SSL servers and authenticate messages from them. It allows each party to define  
18 its own trust relationship with the other business parties in the hierarchy and with other  
19 entities, including public CAs, within boundaries that are set hierarchically.

20

21           The invention provides a way for the hierarchical structure of business  
22 relationships to be incorporated into a security system. The party that is directly above

1 another party in the hierarchy has control over the security information of the lower  
2 party--including what kind of third-party entities can be added by the lower party.

3

4 A root certificate of the top-level entity in the hierarchy, the Software  
5 Provider ("SP") in the preferred embodiment, is preferably stored in non-volatile memory  
6 of a computing device at the time of manufacture. Because subsequent SP root  
7 certificates are chained together as described in the Incorporated Disclosures , the  
8 computing device can verify any later SP root certificate by chaining back to the one  
9 stored in its non-volatile memory. (Or, it can verify by chaining back to a more recent SP  
10 root certificate it has stored locally subsequent to time of manufacture.)

11

12 Each of the other parties provides its own root certificate to the party  
13 directly above it in the hierarchy. The higher party includes a fingerprint of the lower  
14 party's root certificate in a digital object, called the Root Security Information Object  
15 (RSIO). This allows a path to be verified through the hierarchy, by matching a lower  
16 party to its root certificate fingerprint.

17

18 Each party can define detailed trust information, including additional  
19 trusted third-party public CAs. Each party generates its own RSIO, which it digitally  
20 signs and passes to the next higher party in the tree. RSIOs are the basic source of trust  
21 information.

22

1 For any party in the hierarchy, a path can be traced back to the top level  
2 party. Each party in the path has an RSIO. When the RSIOs are chained together, that  
3 object is called a Hierarchical Security Information Object (HSIO). The RSIOs of the  
4 parties (chained into an HSIO) are able to authenticate by tracing an unbroken path of  
5 authentication all the way back to the top of the tree, i.e. the Software Provider in the  
6 preferred embodiment. Because the SP's root certificate is locally available to all other  
7 parties, it can verify the SP's RSIO and each subsequent RSIO can also be verified, given  
8 the structure of the RSIOs, as described below.

9

10 *Definitions*

11

12 A "digital certificate" is a non-forgeable, tamper-proof electronic document  
13 that binds an entity's identity to its public key, as is known in the art of public key  
14 cryptography. Public key cryptography is discussed in the Incorporated Disclosures.

1

2           A "root certificate" is a self-signed and self-authenticating digital  
3        certificate.

4

5           An entity's "fingerprint" or "signature" is unique data that another entity can  
6        recognize as genuine but cannot duplicate. It can function as a person's fingerprint or  
7        signature functions in everyday life. In the preferred embodiment, an entity's fingerprint  
8        is a SHA-1 hash of its X.509 version 3 certificate.

9

10          A "client" is any computing device that participates in the system, including  
11        a classical end-user of a conventional network. Examples of a client are a conventional  
12        personal computer or workstation, personal digital assistant, a set-top box, cellular  
13        telephone, or digital pager. In discussions of the preferred embodiment the term "client"  
14        refers to a set-top box used by a customer of an ISP which could be, for instance, a cable  
15        TV service.

16

17          A "party" is one of the entities that is authorized to issue RSIOs.

18

19        *Business Scenario in the Preferred Embodiment*

20

1 For clarity, the invention is described as applied to a business model in the  
2 consumer market, as described below, with the hierarchy having three levels. A sample  
3 business hierarchy is shown in FIG. 1.

4

5 In the preferred embodiment, the party at the top of the hierarchy is the  
6 Software Provider (SP). It provides software that runs on servers and clients of a web-  
7 based TV system.

8

9 The SP has a business contract with one or more Original Equipment  
10 Manufacturers ("OEMs"), for the OEM to manufacture and distribute client and server  
11 devices that use SP's software. The OEM is the owner of the hardware (servers and  
12 clients that run SP's software) used by the lower levels. The OEM is a large national  
13 cable TV company that broadcasts shows. The OEM is the middle level of the hierarchy.

14

15 The OEM contracts with one or more Internet Service Providers ("ISPs").  
16 The ISP provides service to individual customers. The ISP also provides its customers  
17 with OEM client computers running SP software. The ISP is a small local cable  
18 company. The hierarchy can assume many shapes. For example, an ISP may contract  
19 with several OEMs, or an OEM may contract with several ISPs.

20

21 The invention can be practiced with many other business models. The top-  
22 level entity need not be a software provider and need not be affiliated with web-based

1 TV. It can be any entity requiring computer security, including a financial institution, an  
2 insurance company, a retail store, a government agency, etc. Likewise, the lower-level  
3 entities, if any, can be any entities having a business relationship with the other entities.  
4 Currently in the cable television business, it is common for an OEM to also function as  
5 the ISP. The business model can have fewer or more than three levels.

6

7 *Root Certificates*

8

9            Each party in the hierarchy provides a root certificate. The root certificate  
10 is preferably in X509 version 3 format. A schematic depiction of this format is shown in  
11 FIG. 2. Preferably a period of time for which the certificate is valid is stored in the root  
12 certificate in the field that is labeled Period of Validity in FIG. 2. (A party's root  
13 certificate is provided to the party immediately above it in the hierarchy. This higher  
14 party incorporates the root certificate into the as described below.)

15

16            There are three types of root certificates in the preferred embodiment: SP  
17 root certificate, OEM root certificate, and ISP root certificate.

18

19 Chaining of SP Root Certificate

20

21            Being the top authority, the SP root certificates are chained together as  
22 described in the Incorporated Disclosures. Using this locally stored root certificate,

1 subsequent chained SP root certificates can be verified and validated, as described in the  
2 Incorporated Disclosures. Briefly, root certificate chaining is accomplished by placing,  
3 in the current certificate, a digest--obtained by means of a one-way secure hash function-  
4 -of the public key of the next key pair, i.e. the key pair which will replace the current key  
5 pair when the current certificate expires. FIG. 3 illustrates root certificate chaining.

6

7 Revocation of the root certificate is accomplished.

8

9 At the time of manufacture, the most recent and valid root certificate for the  
10 SP is stored in nonvolatile memory of the computing device. When an updated SP root  
11 certificate is received, the computing device stores this most recent root certificate.  
12 (Thus, a later SP root certificate need only be verified to the most recent root certificate  
13 that the computing device has previously stored, which saves time.) However, if the  
14 client system reverts to its initial operating state (for instance because of a system  
15 malfunction resulting in the loss of all data in writable storage), the client will always be  
16 capable of verifying a later root certificate using the root certificate that is stored in the  
17 computing device's nonvolatile memory at the time of manufacture.

18

19 OEM and ISP Root Certificates: self-signed and self-authenticating

20

21 The root certificates of lower level entities (OEM and ISP root certificates  
22 in the preferred embodiment) are just like any public CA certificates: they are self-signed

1 and self-authenticating as known in the art of cryptography. They are not chained  
2 together. To renew or revoke such a root certificate, the certificate is with new key pairs.  
3  
4

5 *Root Security Information Object and Hierarchical Security Information Object*

6  
7 Each party (SP, OEM, ISP) generates its own root security information  
8 object (RSIO). A sample RSIO for an OEM is shown in FIG. 4. The RSIO is digitally  
9 signed by the entity (preferably, by the entity's current root key pair), and preferably  
10 contains a timestamp.

11  
12 The OEM's RSIO and the ISP's RSIO each contains its current active root  
13 certificate. The SP's RSIO preferably contains the SP's entire root certificate chain. That  
14 is, referring to FIG. 4 (which shows a sample OEM RSIO), for an SP RSIO instead of  
15 merely having the root certificate for the SP, the entire chain of root certificates for the  
16 SP is included.

17  
18 A party's RSIO preferably contains an entry for each entity directly below  
19 the party in the hierarchy and can also include a list of the third party CAs that the party  
20 trusts. Each trusted entity (preferably either an OEM, ISP, or third party CA) has an  
21 entry in the RSIO. Each entity is identified by its fingerprint (to save space).

22

1           The trust information for the each trusted entity is given in the RSIO, and is  
2    preferably implemented by a vector of bits. The delegation information for each trusted  
3    entity is given, and is preferably implemented by a vector of bits.

4

5    Trust Vector and Delegation Vector

6

7           Each entity has associated with it a trust vector. Each bit in the trust vector  
8    designates a role the entity may play. Preferably, some bits in the trust vector indicate  
9    things the entity may do. A sample trust and delegation vector is shown in FIG. 5. For  
10   example, bit 0 may indicate that the entity is a CA trusted to issue certificates for SSL  
11   clients, and bit 1 may indicate that the entity is a CA trusted to issue certificates for SSL  
12   servers. There may be different grades of SSL servers governed by different bits.

13

14           The trust bits can also indicate what role a Public CA can play. For  
15    example, some Public CAs may only be trusted to issue certificates for low-security  
16    applications such as personal email, whereas other Public CAs may be trusted to issue  
17    certificates for high-security application such as securities trading or electronic funds  
18    transfer.

19

20           Other bits in the trust vector identify the entity as belonging to a certain  
21    class, which is trusted to do certain acts. For instance, bit 2 may indicate that the entity is  
22    an OEM (and thus trusted to issue OEM RSIOs) and bit 3 may indicate that the entity is

1 an ISP (and thus trusted to issue ISP RSIOs. Other bits may indicate the entity is one of  
2 SP's special business partners such as an SP system software publisher, which is trusted to  
3 do certain acts.

4

5 Preferably, each trusted Entity listed in the RSIO has associated with it a  
6 delegation vector. Preferably, each bit in the delegation vector designates whether the  
7 corresponding trust vector bit may be turned on by the entity next lowest in the RSIO  
8 hierarchy. For instance, the delegation vector in the RSIO for a specific OEM indicates  
9 what bits ISPs of that OEM may turn on. This has the effect that an ISP may reduce the  
10 trust roles the OEM has assigned an entity (by turning off a trust bit) but may not enlarge  
11 the trust roles the OEM has assigned to an entity in the RSIO.

12

13 In addition to enabling the OEM to retain control of the changes that an  
14 ISP may make, the delegation vector enables the SP to define what authority the OEM or  
15 any lower level party has. Thus, the SP can control to some extent what authority all  
16 other parties have by being able to prohibit lower entities authority to take certain actions  
17 by turning off the delegation vector bit for that action.

18

19 *Chaining of RSIOs*

20

21 The RSIO for an entity contains the fingerprints of its children in the  
22 hierarchy. The fingerprint is preferably a hash of the root certificate. That is, the OEM's

1 RSIO contains a hash of the ISP's root certificate, and the SP's RSIO contains a hash of  
2 the OEM's root certificate.

3

4 A chain of RSIO's from the SP's RSIO to OEM's RSIO to ISP's RSIO forms  
5 a Hierarchical Security Information Object. Preferably the chain is formed using the  
6 fingerprint of the root certificate of the next entity in the chain as the link, as shown  
7 schematically in FIG. 6. For instance, the SP RSIO can be linked to OEM1's RSIO by  
8 matching OEM1's fingerprint in the SP's RSIO to the OEM1 identification in OEM1's  
9 RSIO.

10

#### 11 *HSIO Validation*

12

13 In the preferred embodiment, the client obtains updated trust information  
14 via an HSIO. Before the client relies on the trust information in the HSIO, it must check  
15 that the HSIO is genuine and has not been tampered with. An HSIO is a chain of RSIO's  
16 from the client back to the SP. In the preferred embodiment, for a client of ISP1, that is  
17 an ISP of OEM1, the RSIO chain will consist of SP's RSIO--->OEM1's RSIO--->ISP1's  
18 RSIO.

19

20 The client can validate the HSIO by the following procedure set out in FIG.  
21 7. First check the validity date of the ISP RSIO against the current date. If it is a valid  
22 date, then verify the ISP's RSIO by verifying its signature using the ISP root certificate

1 which is in the ISP RSIO. Check that the ISP fingerprint (hash of its root certificate) is  
2 contained in the OEM's RSIO. Check the validity date of the OEM's RSIO, and verify  
3 the OEM signature in the OEM RSIO. Check that the OEM fingerprint (hash of its root  
4 certificate) is contained in the SP's RSIO. Validate the SP's RSIO by the procedure  
5 described in the above and in the Incorporated Disclosures

6

7 If the HSIO passes the checks set out in the previous paragraph, it is a valid  
8 and genuine HSIO.

9

10 *Update of HSIO*

11

12

13

14

15

16 Preferably, the ISP generates new updated HSIOs, because it is the lowest  
17 level in the hierarchy, interacting directly with clients. (However, updating of HSIOs can  
18 be done by another party.) To generate a new HSIO for a given chain, the ISP needs the  
19 current RSIOs of the SP, OEM, and its own RSIO.

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

1           Events that trigger generation of a new HSIO are the issuance of a new root  
2       certificate by any link in the client-ISP-OEM-SP chain, and when the trust information in  
3       any of the RSIOs has changed.

4

5       *Example: Verification of a non-partner SSL server*

6

7           An example use of the invention is set forth here. The SSL protocol is  
8       widely used. It may often be desirable for a client to be able to do a transaction with a  
9       computer using SSL that is not one of the SP's business partners. For example, a client  
10      (cable TV customer) that wants to purchase products over a web-based TV application  
11      may need to exchange information with a financial institution SSL server.

12

13

14

15

16       The client will receive a server certificate, either signed by a CA or else  
17       self-signed, from the third-party server. Suppose server certificate is signed by Verisign  
18       as a public CA. The client must determine whether this CA is trusted to issue a server  
19       certificate.

20

21       In the preferred embodiment, the ISP is delegated authority to designate  
22       trusted SSL servers and to designate CAs trusted to sign SSL server certificates (In  
23       actual application any specific ISP may or may not have such authority depending on  
24       how higher level entities have delegated authority. To check whether an ISP has  
25       authority to designate CAs trusted to sign SSL certificates, the trust-delegation vector of

1 the OEM RSIO entry for this ISP would be checked.) In the preferred embodiment, the  
2 ISP having authority to designate CAs trusted to do so, the client checks the ISP RSIO to  
3 see if Verisign is included as a CA trusted to sign SSL server certificates. (Instead of a  
4 CA signing the server certificate, the server certificate may be self-signed, e.g. by  
5 Citibank. In such a case, the client checks the ISP RSIO to see whether Citibank is a  
6 trusted SSL server.)

7

8 If the CA signing the server certificate (Verisign in our example) is not  
9 authorized to do so in the ISP RSIO, then the client checks the OEM RSIO to see if  
10 Verisign is included as a CA trusted to sign SSL server certificates. (Or, if instead of CA  
11 such as Verisign signing, the server certificate is self-signed, e.g. by Citibank, the client  
12 checks the OEM RSIO to see that Citibank is a trusted SSL server.)

13

14 If no authorization is found in the ISP RSIO or the OEM RSIO, then the SP  
15 RSIO is similarly checked. If this check fails, then the client cannot do a transaction with  
16 this SSL server.

17

18 If authorization is found in any of the RSIOs in the HSIO, then the standard  
19 SSL handshake protocol proceeds.

20

21 *Example: Step-Up Encryption*

22

1       Using strong encryption internationally is strictly regulated by the U.S.  
2       government. However, a trust bit can be designated to control whether a party is not  
3       trusted to use strong encryption. Preferably, this trust bit would be turned off in the SP  
4       RSIO for computing devices where strong encryption is allowed. The respective  
5       delegation bit would also be turned off, so that lower level entities could not enable  
6       strong encryption.

7

8       *Alternative Embodiments*

9  
10      Although preferred embodiments are disclosed herein, many variations are  
11      possible which remain within the concept, scope, and spirit of the invention, and these  
12      variations would become clear to those skilled in the art after perusal of this application.

1

Claims

2

3       1.     A method, including steps of  
4            sending a first certificate from a first entity, said first certificate including  
5     security information regarding at least a second entity, said first certificate including  
6     information authenticating a second certificate from said second entity; and  
7            sending said second certificate from said second entity;  
8            whereby a recipient of said first certificate and said second certificate can  
9     authenticate from information therein a first set of security information to associate with  
10    said first entity and a second set of security information to associate with said second  
11    entity.

12

13       2.     A method as in claim 1, wherein at least one of the following  
14    includes a root certificate: said first certificate, said second certificate.

15

16

17

18

19

20

21

3.     A method as in claim 1, wherein

4        said first certificate includes both an expiration date and information

5        authenticating a third certificate; and

6        said third certificate includes an expiration date other than said expiration

7        date for said first certificate.

1           4. A method as in claim 1, wherein said first certificate includes  
2 information authenticating a certificate from said first entity other than said first  
3 certificate.

4

5           5. A method as in claim 1, wherein said first certificate includes  
6 information authenticating a future intended version of said first certificate.

7

8           6. A method as in claim 1, wherein said second certificate includes  
9 information authenticating a third certificate.

10

11           7. A method as in claim 1, wherein  
12            said second certificate including security information regarding at least a  
13            third entity, said second certificate including information authenticating a third certificate  
14            from said third entity;  
15            and including steps of sending said third certificate from said third entity

16

17           8. A method as in claim 1, wherein said security information includes a  
18 set of authorizations for said second entity.

19

20           9. An article of manufacture, said article including a computer data  
21 signal embodied in readable medium, said readable medium including at least one of the  
22 following: a carrier wave, a memory, or a storage device; said data signal including

1 a first certificate indicating a first entity as its source and including (a)  
2 security information regarding at least a second entity, and (b) information authenticating  
3 a second certificate from said second entity.

4

5 10. An article as in claim 9, including a second certificate indicating said  
6 second entity as its source; whereby a recipient of said first certificate and said second  
7 certificate can authenticate from information therein a first set of security information to  
8 associate with said first entity and a second set of security information to associate with  
9 said second entity.

10

11 11. An article as in claim 9, wherein at least one of the following  
12 includes a root certificate: said first certificate, said second certificate.

13

14 12. An article as in claim 9, wherein  
15 said first certificate includes both an expiration date and information  
16 authenticating a third certificate; and  
17 said third certificate includes an expiration date other than said expiration  
18 date for said first certificate.

19

20 13. An article as in claim 9, wherein said first certificate includes  
21 information authenticating a certificate from said first entity other than said first  
22 certificate.

1

2           14. An article as in claim 9, wherein said first certificate includes  
3 information authenticating a future intended version of said first certificate.

4

5           15. An article as in claim 9, wherein said second certificate includes  
6 information authenticating a third certificate.

7

8           16. An article as in claim 9, wherein  
9                   said second certificate including security information regarding at least a  
10                  third entity, said second certificate including information authenticating a third certificate  
11                  from said third entity;  
12                  and including steps of sending said third certificate from said third entity

13

14

15

16           17. An article as in claim 9, wherein said security information includes a  
17                  set of authorizations for said second entity.

16

17

1

Abstract of the Disclosure

2 The invention provides a method and system for secure data transfer and  
3 dynamic definition of trustworthiness of various entities by multiple parties in a hierarchy  
4 tree or graph structure. The invention uses digital certificates. Each party in the business  
5 hierarchy can control and define various trust information including trustworthiness and  
6 delegation authority for the entities it deals with. The ability of a party to redefine or add  
7 trust information is controlled by the parties with which it has a relationship that are  
8 above it in the hierarchy. Trust vectors and delegation vectors are used to store this  
9 information. Each party can add trusted third parties to a security object without  
10 compromising the integrity of security objects already issued. A sequence of security  
11 objects including digital certificates can be modified without compromising the original  
12 digital certificates in those security objects.

13

14

FIGURE 1

Sample Business Hierarchy

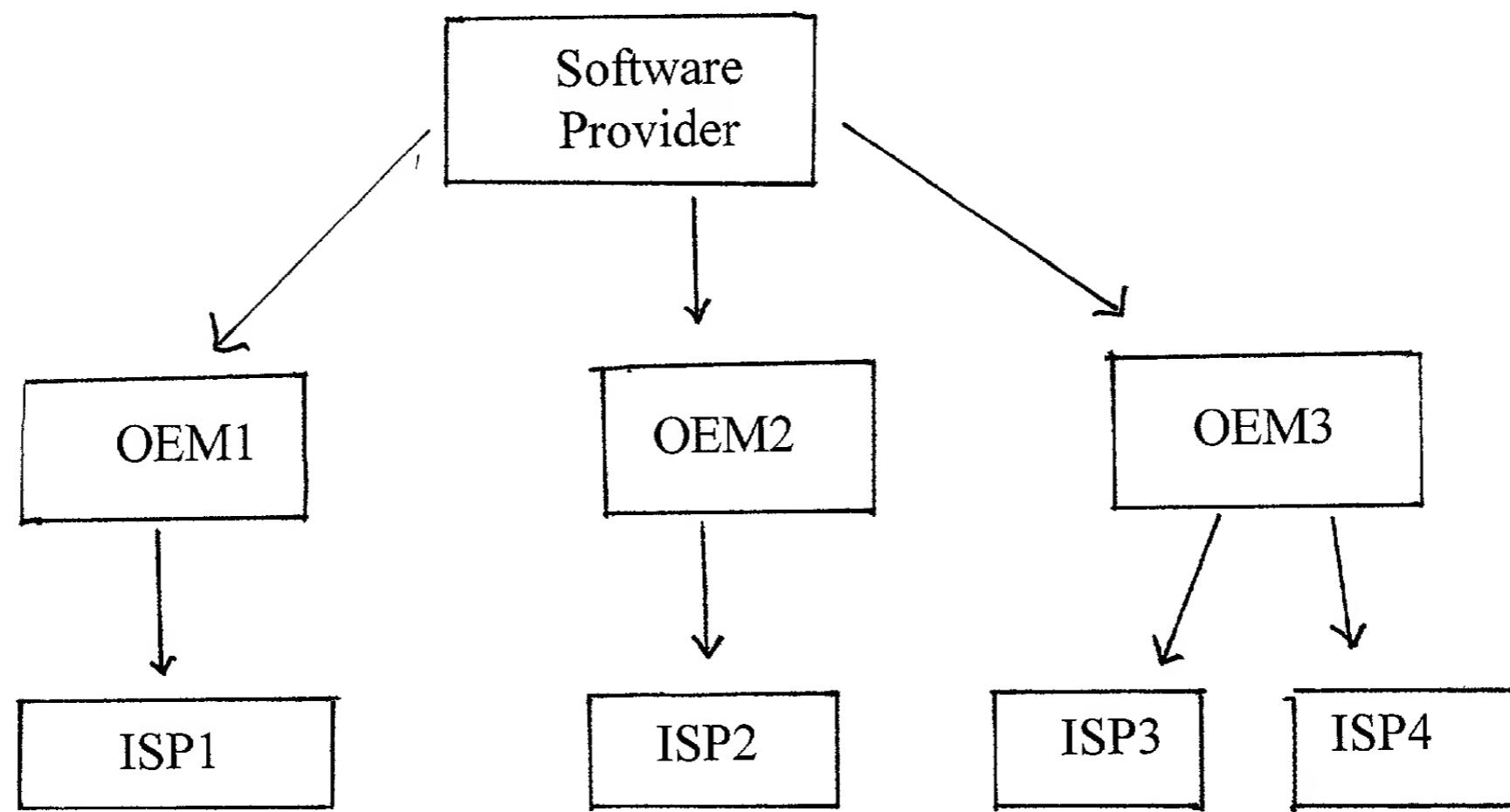
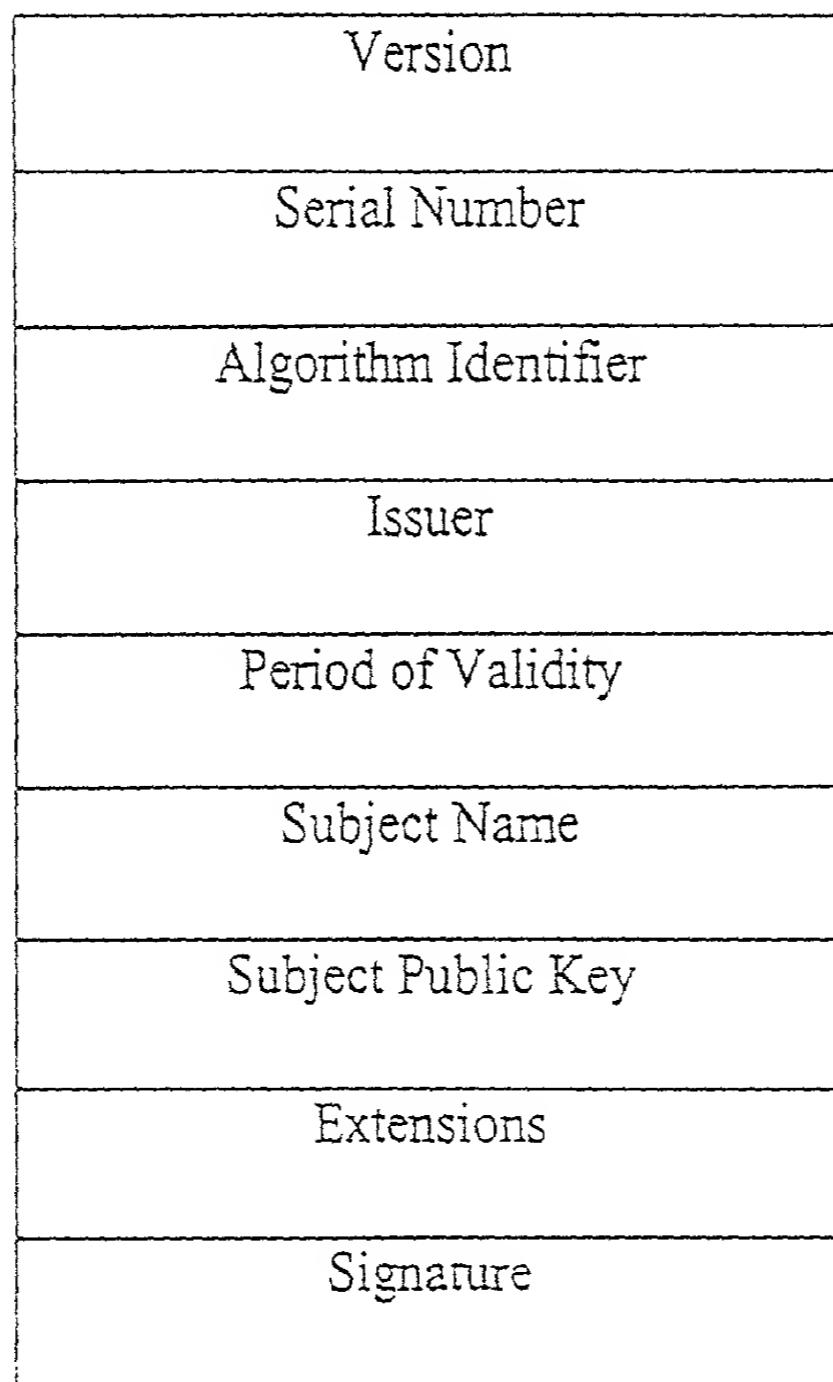


Figure 2

General Format of X509 Version 3 Certificate



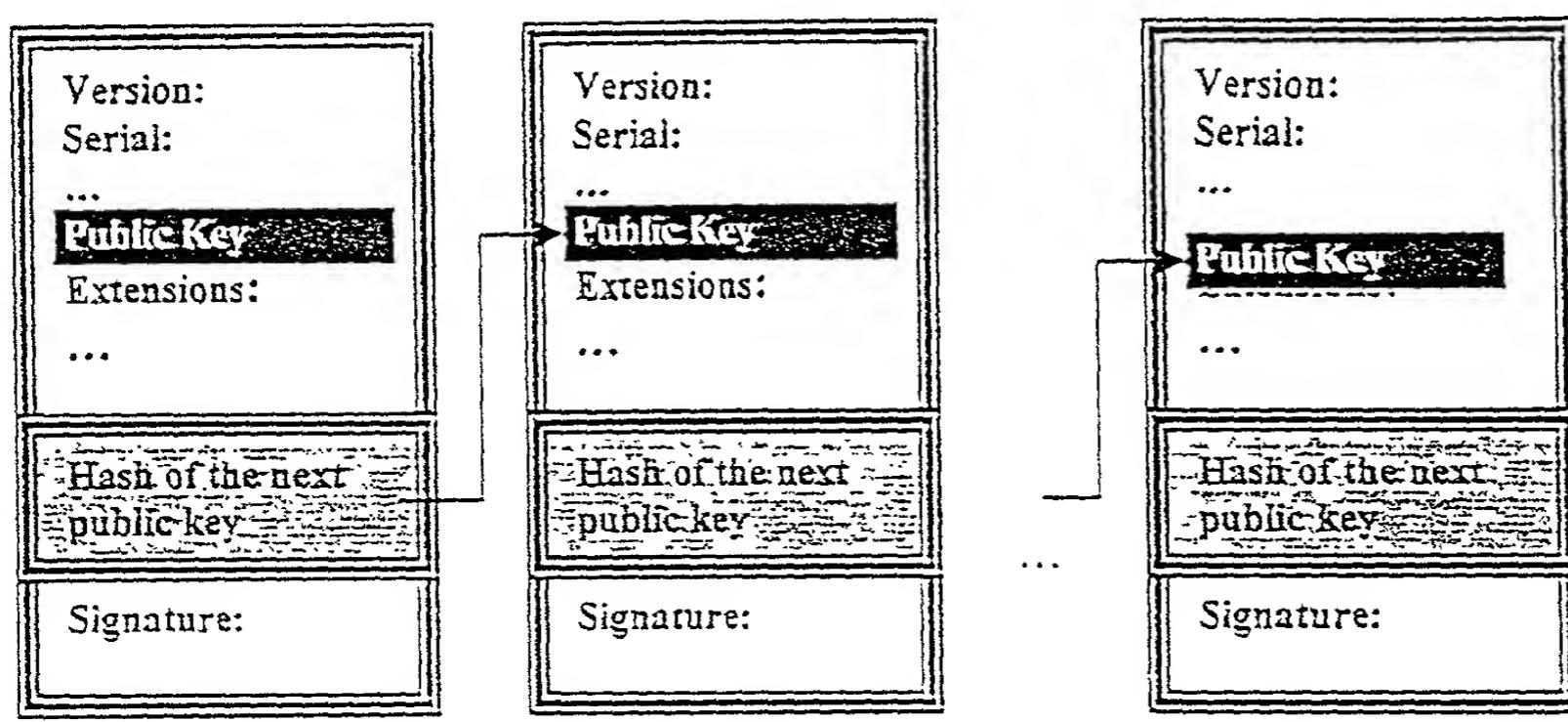


FIG. 3 Root Certificate Chaining

FIG. 4

## SAMPLE OEM RSIO

OEM Root Certificate		
(note: For an SP RSIO the entire chain of SP Root Certificates would be included. For an ISP RSIO the ISP Root Certificate would be included.)		
(Trusted Entity's Identity)	(Trust Information)	(Delegation Information)
Entity_1 Fingerprint	Entity_1 trust information	Entity_1 delegation information
Entity_2 Fingerprint	Entity_2 trust information	Entity_2 delegation information
...	...	...
Entity_m Fingerprint	Entity_m trust information	Entity_m delegation information
CA_1 Fingerprint	CA_1 trust information	CA_1 delegation information
CA_2 Fingerprint	CA_2 trust information	CA_2 delegation information
...	...	...
CA_n	CA_n trust information	CA_n delegation information
Timestamp		
Signature		

**FIG. 5**  
**SAMPLE TRUST-DELEGATION VECTOR**

<b>BIT</b>	<b>DESCRIPTION</b>
0	CA trusted to issue certificates for SSL clients
1	CA trusted to issue certificates for SSL servers
2	CA trusted to issue certificates for SP clients
3	CA trusted to issue certificates for SP servers
4	CA trusted to issue certificates for SP system software publishers
5	CA trusted to issue certificates for SP application software publishers
6	CA trusted to issue certificates for step-up encryption servers
7	Entity trusted as OEM, can issue OEM RSIOs
8	Entity trusted as SP, can issue SP RSIOs
9	SP server instance
10	SP system software publisher
11	Application software publisher

FIG. 6

Schematic of Hierarchical  
Security Information Object

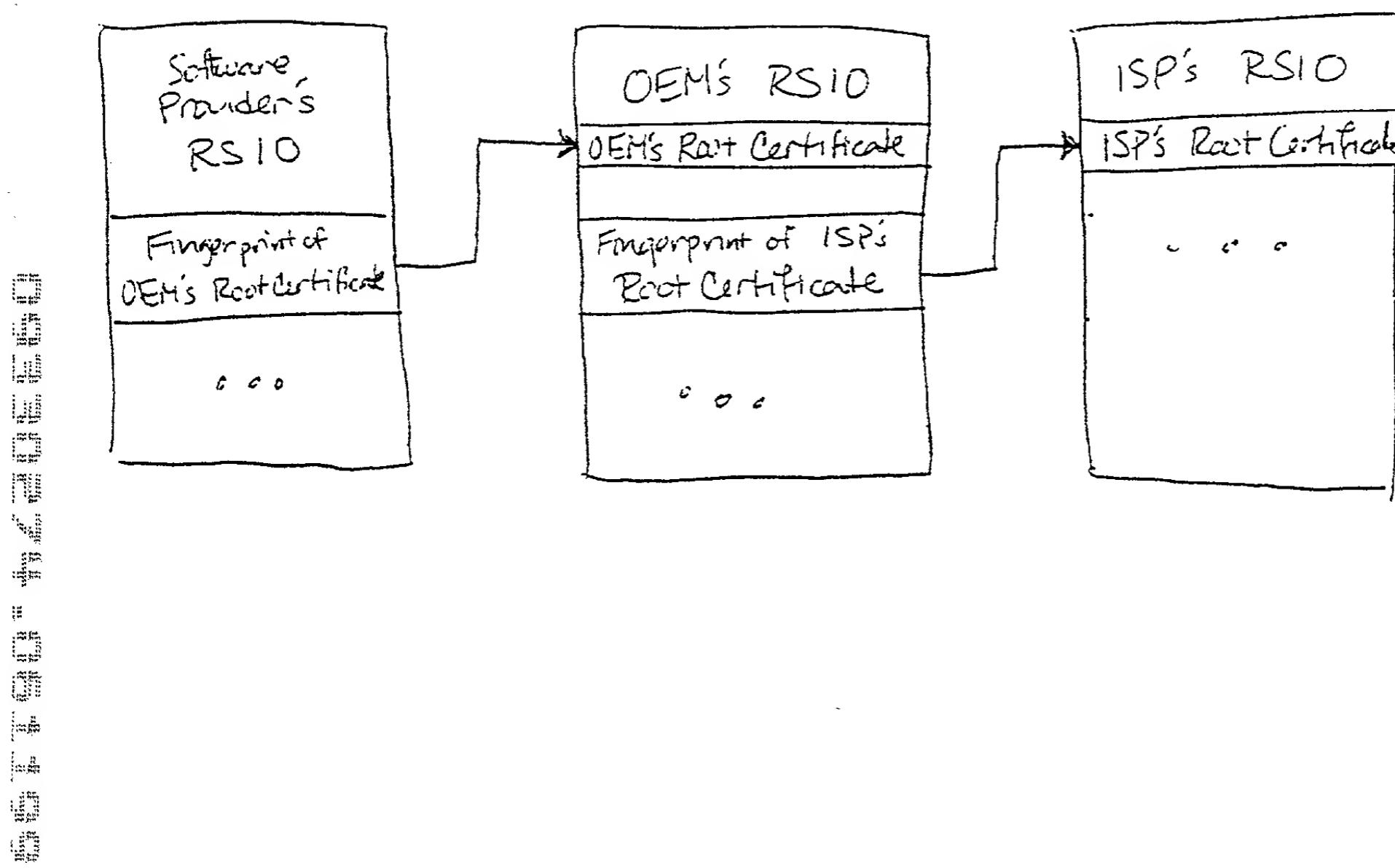


FIG. 7A  
Validation of an HSIO by ISP client

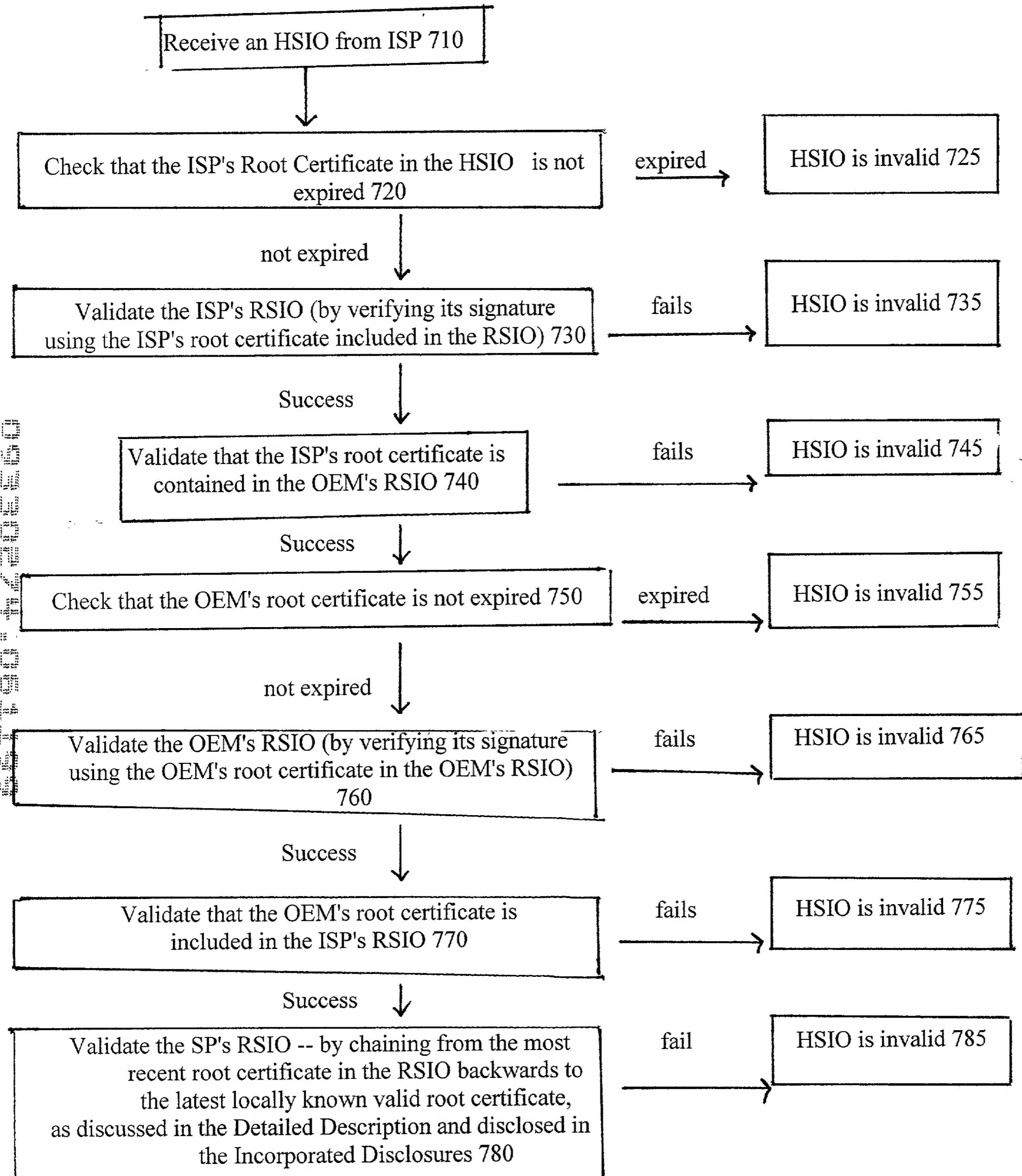


Fig. 7A



success

HSIO is valid 790

NCI-061  
Fig. 7B

FIG. 8  
Authentication of an SSL server certificate  
from non-partner SSL server

